JCA-NET セミナー：監視・検閲との長い闘い—電子フロンティア財団 (EFF) とは

前回紹介した APC(進歩的コミュニケーション協会) が、グローバルサウスに焦点をあてインターネットの草創期から活動してきた団体だとすると、今回紹介する電子フロンティア財団 (EFF) は米国を拠点に、インターネットの初期から検閲や監視に一貫して反対してきた非常に影響力の大きな団体です。スタッフ 1000 人を抱え、裁判をいくつもこなし、議会へのロビーイングからコミュニティでのアクションや技術的な対応まで幅広い活動を展開してきました。EFF はこれまで、主に、政府によるインターネットへの規制や検閲、警察による監視捜査など公権力に主要な関心をもってきました。しかし、今、EFF は、その主要な活動領域を民間企業による市民への監視やプライバシー侵害の問題にも向けはにてています。日本には残念ながら EFF のようなインターネットを主要な活動領域とする市民的自由や人権問題に取り組む団体はありません。最近の EFF の活動、インターネットの本拠地アメリカで何が起きているのかについて紹介しながら、日本の反監視運動の課題を探ります。

電子フロンティア財団ウエッブ

https://www.eff.org

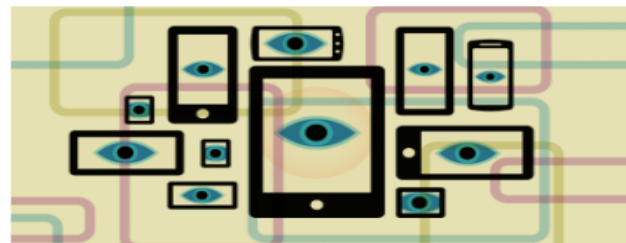
The leading nonprofit defending digital privacy, free speech, and innovation.

FEATURED UPDATE

DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers

The Computer Fraud and Abuse Act (CFAA), the notoriously vague anti-hacking law, is long overdue for major reform. Among many problems, the CFAA has been used to target security researchers whose work uncovering software vulnerabilities frequently irritates corporations (and U.S. Attorneys). The Department of Justice (DOJ) today announced a new policy under which it will not bring CFAA prosecutions against those engaged "solely" in "good faith" security research. It's an important step forward that the DOJ recognizes the invaluable contribution...

FEATURED UPDATE

We Finally Have a Federal Fiber Broadband Plan

FEATURED UPDATE

How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now

https://www.eff.org

EFF の歴史

1990 年 7 月、言論とプライバシーに対する基本的な脅威に対処するために設立された

初期の課題は政府の検閲との闘い

- スティーブ・ジャクソン・ゲームズの訴訟

電子メールは少なくとも電話と同程度の保護に値すると、初めて裁判所が判断

- Bernstein v. U.S. Dept. of Justice

書かれたソフトウェアコードは憲法修正第 1 条で保護される言論であると、史上初めて判決

暗号に関する輸出コントロール法は、憲法で保護されたバーンスタインの言論を禁止するものであり、バーンスタインの憲法修正第 1 条の権利を侵害するものであるとの判決

EFF の歴史

現在

- 特定の強力な企業が、オンラインでの言論を封じ、消費者に新しいイノベーションが届くのを妨げ、政府の監視を促進しようとしています。私たちは、政府による権力の乱用に対抗するのと同様に、企業の行き過ぎた行為に対抗
- オンライン上で個人がプライバシーとセキュリティを保護するのに役立つテクノロジーを開発し、EFF の技術者がそれを構築して、誰でも使えるように一般に公開
- 知的財産権に関する提案に見せかけたデジタル検閲法案を撃退し、企業にユーザーを監視させる試みに反対し、政府の監視を抑制する改革法案を支持
- 人権と憲法上の権利の双方を尊重するグローバルなデジタル環境を構築するために、世界中の支持者とともに仕事

2020 年のレポート

- 位置追跡と感染者接触通知広範な COVIĐ 電話追跡アプリへの抵抗
- デジタルアイデンティティと "ワクチン用心棒 "
- COVIĐ データの確保 変化する地盤の上でデータプライバシー規則を構築する
- COVIĐ-19 とデジタル格差

2020年のレポート

- AMAZON RING 官民一体となった監視とデジタル過剰捜査に立ち向かうために
- WILIAMES V. SAN FRANCISCO

  デモ参加者の監視と闘う
- a theory of disciplinary tech 監視の常態化に対する反撃
- student プライバシー学校と家庭での急激な監視から生徒を守るために

2020年のレポート

- youtube コンテンツ id 独立系クリエイターのオンライン表現に期待
- pride and online expression LGBTQの声をオンラインで高揚させる

2020年のレポート

財政基盤

収入　約1300万ドル

- 世界中の38,000人以上の会員からの寄付
- 資金の90%以上が個人からのもの
- その半数以上は1,000ドル以下の寄付

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

私は2年以上前、人種や移民の正義に関する専門知識を、政府の監視に対する闘いに生かすことを目標に、EFFに参加しました。そして、これらの問題は、ジョージ・フロイドの殺害をきっかけに米国史上最大の抗議運動が起こった2020年の夏に、最重要視されるようになりました。

EFFは、オンラインや街頭で、黒人の命のために立ち上がるための取り組みをすぐに強化しました。私たちは、抗議活動への参加、特に抗議活動における携帯電話の監視に関する「Surveillance Self-Defense」ガイドなどの技術的リソースを提供しました。私たちはナショナル・ローヤーズ・ギルドと協力して、彼らのリーガル・オブザーバー・プログラムのために、抗議活動における可視および不可視の監視を観察するためのガイドを作成しました。私たちはこの重要な憲法修正第1条の権利を支持するために長年にわたって提出した法廷用準備書面に基づいて、警察を安全かつ合法的に記録する権利に関する助言を公表しています。そして、法執行機関が抗議活動を監視するためにどのように監視テクノロジーを採用しているかを明らかにするために、情報公開法を利用しました。

Saira Hussain

STAFF ATTORNEY

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

2020年7月、私たちはサンフランシスコの準政府機関であるいくつかのビジネス改善地区（BID）に公文書公開請求を行い、そのうちのいくつかは、街の何百ブロックもの生活を撮影する監視カメラのプライベートネットワークを備えていることが判明しました。サンフランシスコの中心部に位置するユニオン・スクエアBIDは、その回答の中で、サンフランシスコ警察（SFPD）に抗議活動を監視するために、400台以上のカメラのネットワークに1週間ライブでアクセスすることを許可したことを明らかにしました。

このライブ監視は、2019年にサンフランシスコ監督委員会のほぼ全会一致で制定された市の監視テクノロジー条例に違反するものでした。この条例は、SFPDのような市の機関が、コミュニティの声を聞く機会を与える公開プロセスを経て監督委員会の許可を最初に得ずに監視テクノロジーを取得または使用することを禁じています。EFFは、ホープ・ウィリアムズ、ネイサン・シアード、ネストル・レイズの3人の黒人活動家の弁護団の一員として、サンフランシスコ市警の監視テクノロジー条例違反に対して訴訟を起こしています。この訴訟は、サンフランシスコに条例を施行し、サンフランシスコ警察を法の下に戻すよう求める裁判所命令を求めるものです。

私がホープやネイサン、ネスターのような抗議者のために闘うのは、正義のための運動が長年にわたり政府の執拗な監視の対象であり、監視テクノロジーの進歩によってさらに侵襲的なものとなっているからです。私たちは、抗議者が自由に発言する権利を守らなければなりません。ホープの言葉を借りれば、「私たちは警察の監視を恐れずに組織化し、発言し、行進する権利がある」のです。

Saira Hussain

STAFF ATTORNEY

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

昨年、EFFは、日常生活における監視を常態化させている消費者や企業のソフトウェア、アプリ、デバイスの拡大カテゴリーに焦点を当てました。私たちはこれを「規律のテクノロジー」と呼び、監視が最も受け入れられ、権力の不均衡が常態化している場所に典型的に現れます。職場には「ボスウェア」、学校には遠隔試験監督、ソーシャルメディア監視、デバイス監視、家庭や近隣にはストーカーウェア、「キッズウェア」、家庭用監視システムなどがあります。

私は5年前、図書館情報学修士号を取得してEFFに来たときから、このような様々なテクノロジーの関係について考え続けてきました。この数年間、最も印象に残っているのは、フェミニストのプライバシー理論に関する講義です。家庭や家族といった最も「プライベート」な領域は、女性に対する暴力が外部からの監視や介入から最も遮断される場所でもあるという発展的な考えを、この授業で正式に学びました。私たち学生の課題は、弱者や疎外された人々がどこで「間違った時に間違った種類のプライバシー」を持つのかを理解し、わざわざ権力者をかばうようなことのないプライバシー価値を思い描くことでした。データサイエンスの宿題や問題集に追われながら、このような倫理の授業を受けると、そもそもなぜ学校に通っていたのかが思い出されます。

それは、テクノロジーがいかに力の不均衡を悪化させるかを学び、その均衡を取り戻すための運動に参加するためです。

そして、これこそが、EFFが規律のテクノロジーに関する新しい公教育キャンペーンで行っていることなのです。

Gennie Gebhart

ACTIVISM DIRECTOR

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

広範な監視を受け入れるだけでなく、自分たちの職場や学校、家庭を率先して監視だらけにするよう、私たちを説き伏せるのは、監視経済の巧妙な手口と言えるでしょう。課題は、ユーザーの選択、透明性、厳格なプライバシーとセキュリティの基準など、典型的な権利擁護の叫びが、監視が要点である場合には完全な解決策にならない、ということです。規律のテクノロジーの蔓延を解決するには、より強力な手段が必要です。私たちは、規律テクノロジーのメーカーが資金提供を受けて、同僚や学生、友人、家族、隣人を口実や強制、力づくでスパイすることは、いかなる人物や組織にとっても許容できる行動だという考えが広まっていることに反対する必要があるのです。

規律のテクノロジーが集団として隆盛を誇るのは、その定義が非常に難しく、またある人々にとっては正当化するのがとても簡単だからなのです。しかし、規律のテクノロジーが実際にその宣伝された目的を達成することができると信じる根拠はありません。ボスウェアはビジネスの成果を決定的に向上させるものではないし、学校の監視が効果的な安全対策やカンニング防止対策になるという独立した証拠もありません。また、自分のパートナーや子供をデジタルでストーキングすることは、健全な関係とは正反対であることは明らかです。監視を利用して権力者にさらなる権力を与えることが目的なら、規律のテクノロジーは「うまくいく」と言えるかもしれません。しかし、その対象者や社会全体にとっては大きな犠牲を伴うものです。

Gennie Gebhart

ACTIVISM DIRECTOR

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

私が最も恐れているのは、次の世代が家庭や学校で常に監視されながら成長し、職場や人間関係で大人と同じように監視されても、微塵も感じなくなることです。同僚のエヴァは、この恐ろしいテクノロジーのライフサイクルを "ゆりかごから墓場まで"の監視と呼んでいます。しかし、私が希望を持ち続けられるのは、EFFに毎日寄せられる、親や子供、労働者や家の所有者からの電話やメールです。彼らは、自分たちの生活の様々な分野に忍び寄るテクノロジーについて、何かがおかしいと感じ、戦う準備を整えているのです。

一度にひとつの規律のテクノロジーだけをターゲットにしても、うまくいきません。それぞれのユースケースは、同じような衝動や 監視の傾向を反映した、同じヒドラの別の頭なのです。例えば、ストーカーウェアのアプリに絞って対抗し、一方、キッズウェアやボスウェアをそのままにしておくと、基本的なテクノロジーは、それを悪用しようとする人たちが堂々と利用できるようになります。

そのため私たちは、アンチウイルス会社やアプリストアに対してスパイウェアをより明確に認識するよう要求し、悪用されるケースを想定した設計を企業に求め、監視ベンダーの空約束に誘惑されてしまう人々や機関を指導するなど、このテクノロジー群全体への対処に取り組んでいるのです。私たちの仕事は大変なものですが、その一方で、私たちを支えてくれる支援者のコミュニティも広がりつつあります。そして、このような状況を少しでも改善するために、私は毎日仕事に出かけています。

Gennie Gebhart

ACTIVISM DIRECTOR

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

デジタル・アイデンティティと "ワクチンの用心棒"

デジタルヘルスの証明書のリスクを精査する

Alexis Hancock

DIRECTOR OF ENGINEERING, CERTBOT

避難生活が実施されている中、パンデミックへの対応は、私たち全員がその都度学ばなければならないものでした。完全に屋内にとどまる人もいれば、Target でトイレットペーパーを買い占める人もいました。最初のパニックの中で、感染者を追跡し、COVID-19 の検査結果を記録し、健康な人と感染者、ワクチン接種者と未接種者を区別することを約束するテクノロジーが開発されました。

私たちが自宅でのリモートワークに慣れるにつれ、EFF のチームはこれらの提案が一体何であったかを掘り下げていきました。政府がワクチンの流通を管理する以前に、さまざまな企業、グループ、組織がデジタル COVID-19 証明書を作成する作業に飛びつきました。最初の提案では、「免疫パスポート」という言葉が使われました。デジタル・トークンで「免疫」を保証することはできないし、「パスポート」という名称は、根拠のない健康基準によって自分の行動が左右されるような近未来を想像させるものである、という問題点はすぐに明らかになりました。

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

EFFにとって、国民IDの仕組みやその潜在的な誘因に直面するのは今回が初めてではなく、デジタルIDに伴うさまざまなリスクについて警鐘を鳴らす用意がありました。この1年を通じて、私たちの立場は、特に「ワクチン用心棒」に強く反対してきました。EFFと私たちのコミュニティは、特に恐怖とパニックの時代において、「一時的な」監視手段が長期的な結果をもたらす危険性について、熟知しています。パンデミックの始まりから終わりまで社会を巻き込むことは、追跡やデータ漏えいのリスクにさらされる機会を拡大する結果になってはならないのです。今は、人々をさらに疎外する可能性のある実験的なテクノロジーを展開する時ではなく、データプライバシー法のようなセーフガードを作る時なのです。

私たちにはやるべきことがあるのです。CLEARのような企業は、民営化されたTSAプレチェックのようなものとしてすでに空港で存在感を示しており、"ヘルスパス"を開発しました。

この「ソリューション」が導入された範囲は、そのタイミングを考えると公衆衛生対策というよりも、企業に対してデジタルIDを日常的に交換するための第一のプラットフォームとしての座を射止めることに重点が置かれていました。ニューヨーク州は、IBMのデジタルヘルスプラットフォームと粗末なプライバシーポリシーで構築された「Excelsior Pass」を導入しました。

Alexis Hancock

DIRECTOR OF ENGINEERING, CERTBOT

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

最近では、カリフォルニア州が「デジタル・ヘルス・レコード」を発表しました。多くの「ワクチンパスポート」は、現在、包括的な「健康パス」、さらにはデジタル運転免許証として自らを売り込むように進化しています。デジタル・アイデンティティとその意味合いに関する EFF の分析を共有することで、健全な時代と危機の時代の両方において、私たちを方向付けることができるデータ・プライバシー法のガイドラインを設定することができればと願っています。

デジタル経路の IĐ を求める声は、米国でも国際的にも続いています。しかし同時に、デジタル上の不公平は解消されず、企業はあまりにも不十分な説明責任で運営され、デジタル上の「問題を探し求める解決策」はあまりにも頻繁に、結果に対する素朴な感覚しか持ち合わせていないのです。その意図が善意であれ、悪意であれ、あるいは中途半端であれ、今大切なのは意図ではなく、インパクトなのです。これらの製品の多くは、危機的な状況の中で展開されたため、その潜在的な影響は、それに値する精査を回避されてきました。

EFF は必要な精査を行い、皆さんの協力のもと、デジタルヘルス認証に関する議論が続くよう、警戒を怠りません。

Alexis Hancock
DIRECTOR OF ENGINEERING, CERTBOT

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

位置追跡と曝露通知

行き過ぎたCOVIDスマホ追跡アプリに抗う

Adam Schwartz

SENIOR STAFF ATTORNEY

2020年3月にCOVID-19が発生したとき、私は本当に怖かった。私たちは皆、発病した人たちを知っていました。社会的な距離の取り方は、かつてないほどの孤立をもたらしました。我が家では、特に10代の子どもたちが辛かったです。

「危機を技術で乗り切ろう」という提案はすぐさま実現しました。私たちの多くは携帯電話を持ち、それによって常に私たちの動きやその他多くのことを監視しています。新しい健康アプリをインストールして、誰とどこに行ったかを記録してはどうだろう。そうすれば、誰かが感染した場合、その人が近くにいた人をすぐに特定し、検査することができるのです。これは、伝統的な公衆衛生対策であるコンタクトトレースと類似しており、これは、感染者にインタビューを行い、その人が誰と一緒にいたかを知るものです。なぜ、この手作業を自動化しないのか？提案者は、これが感染とロックダウンの両方を回避するのに役立つと主張しました。

EFFはすぐにその仕組みを調べました。しかし、私たちはそれを見て気に入りませんでした。そして、警告を発したのです。私たちは、活動家、弁護士、技術者からなるワーキンググループを結成しました。私たちは、世界中で実装・提案されているCOVID携帯電話追跡アプリを綿密に調査しました。新しい監視テクノロジーは、危機の最中には聞こえが良いかもしれませんが、約束された安全上の利益を達成することはほとんどなく、私たちの市民的権利や自由を損なうことが多く、危機が去った後に取り除くのは至難の業なのです。

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

ある提案は、携帯電話のGPSと携帯サイト位置情報（CSLI）を通じて私たちの動きを追跡するものでした。このような位置情報では、二人がウイルスに感染するほど接近しているかどうかを示すには不十分です。CĐCは6フィートの社会的距離を推奨していますが、CSLIは半マイルまで、GPSは16フィートまでしか正確ではありません。しかし、CLSIとGPSは、位置情報のプライバシーを侵害し、例えば、労働組合の集会に参加したか、BLMの集会に参加したかを明らかにするのに十分な精度を備えているのです。もう一つの方法は、携帯電話のBluetooth信号強度を測定することによって、他人との近接性を追跡することです。2人の人間が互換性のある近接アプリをインストールし、ウイルスを感染させるのに十分な距離に近づくと、彼らの携帯電話アプリはデジタル・トークンを交換することができます。その後、一方が感染した場合、もう一方に通知することができます。

Adam Schwartz

SENIOR STAFF ATTORNEY

近接トラッキングは、ギリギリのところで役に立つかもしれないし、役立たないかもしれません。数フィート離れたところに立っている二人が壁で隔てられているような場合、近接トラッキングは過剰な効果を発揮するでしょう。特に、低所得者、住居のない人、高齢者など、COVIĐの影響を最も受けやすい人々の間では、スマートフォンを持っていない人が多くいます。さらに、多くの人は接近型アプリを使うことはありません。おそらく最も重要なことは、検査、手動での接触者追跡、隔離中の患者へのサポート、社会的距離の取り方、マスクの着用、そして現在のワクチン接種といった従来の公衆衛生対策の必要性を、どのアプリも満たすことができない点です。

2020 レポート：ウィリアムズ対サンフランシスコ 抗議者のために闘う

接近型アプリは、プライバシーのために設計されなければなりません。残念ながら、多くはそうではありません。中央集権的なモデルでは、政府はすべての接近データにアクセスでき、それをある特定の人々と照合することができます。これはデジタル上の権利を危うくします。しかし、多くの国がこの方式を採用しています。

より良いアプローチは、GoogleとAppleのExposure Notification（GAEN）です。これは、特定の個人との関連付けが困難な、一時的でランダムな識別子のみを収集するものです。また、GAENはこれらの識別子をユーザーの携帯電話に保存します。もしユーザーが陽性と判定された場合、その識別子を一般にアクセス可能なデータベースにアップロードするかどうかを選択することができます。GAENに対応したアプリは、アメリカの多くの州や外国の公衆衛生局がスポンサーになっています。もちろん、参加は任意でなければなりません。

パンデミックの初期に、EFFが携帯電話を位置追跡や 中央集中型の接近型追跡のために使うことを避けるよう、世論を動かすことに貢献したことは、私の誇りです。新しいテクノロジーを迅速に評価し、政策立案者、開発者、そして一般の人々に、予期せぬ危険について啓蒙することが、私たちの仕事なのです。

私の子どもたちは、ロックダウンから解放されるのを楽しみにしています。EFFの仕事のおかげで、どこに行くにも持ち歩く携帯電話に組み込まれた、侵襲的な新しい監視システムをどうやって解体するかについて悩まず、そうできるのです。